UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA

LISA GLADWELL AND SHARON MORGAN,
on behalf of themselves and all others similarly situated,

Plaintiffs,

Civil Action No. 5:17-cv-04061

v.

EQUIFAX. INC.,

SERVE:
Corporation Service Company
209 West Washington Street
Charleston, WV 25302

EQUIFAX INFORMATION SERVICES, LLC, and

SERVE:
Corporation Service Company
209 West Washington Street
Charleston, WV 25302

EQUIFAX CONSUMER SERVICES LLC,

SERVE:
WV Secretary of State
Equifax Consumer Services, LLC
1550 Peachtree Street, NE
Atlanta, GA 30309

Defendants.

CLASS ACTION COMPLAINT

COME NOW Plaintiffs, Lisa Gladwell and Sharon Morgan on behalf of themselves and all other consumers similarly situated, by counsel, seek judgment against Defendants Equifax. Inc., Equifax Information Services, LLC ("EIS"), and Equifax Consumer Services LLC ("ECS") (collectively, "Equifax"), and state as follows:

I. PRELIMINARY STATEMENT

1. This is an action for damages, costs, and attorneys' fees brought pursuant to common-law negligence. Defendants negligently allowed the fraudulent procurement of the critical private information of Plaintiffs' and Class Members' consumer report files, and failed to disclose the fact of such procurement from plaintiffs.

2. Defendants operate together as a unified consumer reporting agency ("CRA") to prepare and furnish consumer reports for credit and other purposes. Equifax's databases contain a treasure trove of valuable information about nearly every American adult—account numbers and payment histories, Social Security numbers, names and aliases, birthdates, addresses, employment histories, and the like—that Equifax collects and sells to businesses that extend credit, loan money, sell insurance, and grant employment, among numerous other activities.

3. Defendants obtain the largest portion of its vast store of data independently and without consumers' consent or knowledge. Put differently, consumers rarely turn data over to Equifax knowingly and willingly—most of the data Equifax possesses it obtained from sources other than the consumers themselves.

4. By now, the Court has already read of the "Equifax breach", and possibly Defendants' response to it. In May of 2017, and likely earlier, unknown individuals electronically accessed Equifax's databases without Defendants' knowledge, gaining access to information about

approximately 143,000,000 Americans.[1] Ironically, the identity thieves entered Equifax's systems through the Internet portal it uses to receive consumer disputes of identity theft and other credit inaccuracies,[2] and then accessed collateral database information from there, including Defendants' core consumer contact database, "ACIS."[3]

5. Defendants have disclosed generally that the fraudulent users procured consumers' names, Social Security numbers, birthdates, addresses, and driver's license numbers.[4] The breach lasted for months and, although Equifax knew about the security vulnerability in May, and the breach itself in July at the latest, it sat on this information until September 8, 2017.

6. While Equifax has revealed that the breach took place, it has been anything but transparent. It has yet to identify the specific individuals affected, reveal exactly what information was taken or learned by the hackers and when, or take any preventative steps other than to alert consumers who are able to navigate its website that they "may" be affected by the breach, often with inconsistent results. For a company that traffics in electronic information of such a sensitive and specific nature, this is unacceptable.

7. Plaintiffs include West Virginia consumers regarding whom Defendants possessed information protected by the federal Fair Credit Reporting Act, which was thereafter unlawfully procured by identity thieves between March and July 2017.

8. Plaintiffs assert a negligence claim for themselves and all other West Virginia consumers. Equifax possessed significant, important financial data about them but failed to

---

[1] *See* https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.
2 Equifax had created that portal as a means to fully automate its "reinvestigations" of consumer disputes and – in theory – avoid the expense of having live human beings oversee that process and obligation.
3 "ACIS" is Equifax's acronym for its "Automated Consumer Interview System".
4 https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

exercise the standard of care required of an entity with such "grave responsibilities" that come along with the right to store and sell such information. 15 U.S.C. § 1681. Because of that failure, Equifax permitted unauthorized access to Plaintiffs' and Class Members' personal information, which in turn caused them to suffer not only actual harm caused by the stress of not being able to know what was accessed and how it will be used by the perpetrators of the breach, but also the risk of harm that their identities will be stolen, accounts improperly accessed, or credit injured, among other potential harms.

II. JURISDICTION

9. The Court has diversity jurisdiction as to all Plaintiffs and all Class Members pursuant to 28 U.S.C. § 1332(a) as all Plaintiffs seek to recover damages in excess of $75,000 individually for actual damages and every Plaintiff is diverse from Defendants.

10. The Court also has diversity jurisdiction pursuant to 28 U.S.C. §1332(d), as none of the Plaintiffs are from the same state as Defendants, more than two-thirds of the putative class resides and is legally domiciled in a state other than Georgia or that of Defendants, there are at least tens of thousands of class members and the total amount that will be recovered in damages will exceed $5 million.

11. Defendant Equifax is a corporation headquartered in Atlanta, Georgia, and Plaintiffs and all consumers embraced by the Class definition below reside in the Southern District of West Virginia.

12. Defendant Equifax is subject to personal jurisdiction in the Southern District of West Virginia, by virtue of the business it conducts in the Division. Further, it deliberately and specifically availed itself of the benefits of West Virginia and caused direct injury to West Virginia consumers, including the Plaintiffs, in West Virginia.

13. The Court also has subject matter jurisdiction as each Plaintiff suffered real and definite harm. Defendants confirmed that the core personal information maintained by Equifax was furnished to and procured by criminal data thieves. They will now spend the rest of their lives worried about, fearful of and having to expend time and money to prevent credit, criminal, tax filing and other identity theft events. Further, Plaintiffs also suffered tangible injury in the value of the credit monitoring service they were denied. And all Plaintiffs suffered injury in the denial of the substantive rights the FCRA was intended by Congress to afford.

III. PARTIES

14. Plaintiffs are each natural person and "consumers" as defined by the FCRA.

15. Each Plaintiff named herein has reason to believe, based upon the public reports of the Data Breach, its scale, and upon information provided by Equifax via its website, that her personal identifying information ("PII") was taken during the Data Breach.

16. Plaintiff Lisa Gladwell is a resident of Lewisburg, West Virginia. On or about September 15, 2017, Plaintiff Gladwell visited the Equifax website which stated to her that she may be a victim of the Data Breach. Plaintiff Gladwell has devoted significant time to monitoring her accounts in response to the Data Breach. She was never alerted or advised by Equifax that her consumer report information had been procured as a result of the Data Breach.

17. Plaintiff Sharon Morgan is a resident of Lewisburg, West Virginia. On or about September 18, 2017, Plaintiff Morgan visited the Equifax website which stated to her that she may be a victim of the Data Breach. Plaintiff Morgan has devoted significant time to monitoring her accounts in response to the Data Breach. She was never alerted or advised by Equifax that her consumer report information had been procured as a result of the Data Breach.

18. All three Defendants are both "consumer reporting agencies" and "nationwide consumer reporting agencies" as defined and governed un the FCRA.

19. Defendant Equifax, Inc. is the parent of the two additional Defendants. In prior litigation, it has taken the position that it is not itself a "consumer reporting agency" governed by the FCRA. *See* 15 U.S.C. § 1681a(f) ("The term "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.")

20. But of course, Equifax, Inc. *is* a consumer reporting agency. For purposes of the FCRA, Equifax, Inc. has held itself out repeatedly to consumers, regulators and the public generally as the actual operating entity. The branding, labels and disclosures on the Defendants' consumer website is dominated by "Equifax, Inc." titling. Defendants have held Equifax, Inc. out as the operating and responsible entity.

21. Defendant Equifax Consumer Services, LLC is similarly a CRA. It for monetary fees, regularly engages in part in the practice of assembling and maintaining consumer report information in its operational relationship with Equifax, Inc. and EIS.

22. Defendant Equifax Information Services, LLC is a foreign limited liability company transacting business in West Virginia and maintains a registered agent office in Charleston, West Virginia. At all times relevant to this action, EIS has acknowledged that it is and was a "consumer reporting agency" as defined by the Fair Credit Reporting Act, § 1681a(f).

23. The FCRA, through a rule mandated at § 1681x, expressly prohibits "a consumer

reporting agency from circumventing or evading treatment as a consumer reporting agency" by means of corporate reorganization or structuring.

24. Equifax, Inc. and its subsidiaries – whether or not they observe state law corporate formalities – have eliminated nearly all lines between their different business entities in the collection, maintenance, sharing and furnishing of consumer reporting information. Equifax, Inc., entities such as EIS regularly share FCRA restricted information with sibling entity ECS to market and profit from the sale of consumer identity theft prevention products, including the blurring of legal lines between providing file information under the FCRA versus for private sale to the consumer. Equifax subsidiary TALX Corporation operates as Equifax Workforce Solutions, and with control of acquired-entity eThority and both provides and obtains FCRA-governed consumer information to and from other Equifax entities. Equifax entity Anakam, Inc. integrates Equifax consumer data for sale of its fraud detection and verification products, largely now under the Equifax brand. And, by last example Equifax Mortgage Services operates as a separate entity focused on the mortgage services industry, but also freely shares and uses otherwise FCRA protected data.

25. Further, throughout this breach and post-exposure conduct, the Defendants have operated and acted as one entity and CRA.

26. Here, Equifax, Inc. has used EIS and ECS as dependent and integrated divisions rather than as separate legal entities. The business operations are fully coordinated and shared. Resources are cross-applied without full and complete cost and profit centers. Management decisions at EIS and ECS are made by and through management at Equifax, Inc. And the entities largely hold themselves out as a single uniform business.

27. For purposes of the claims here, these facts are especially meaningful. Data security was shared and the negligence here was directly that of management officials at Equifax, Inc. In fact, it was Equifax. Inc.'s Chief Security Officer Susan Mauldin and Chief Information Officer David Webb who Defendants have fired as a result of the events alleged herein, rather than employees of the subsidiary entities. Equifax, Inc.'s president has directed all matters related to these events. And Equifax, Inc.'s General Counsel was and has remained the Chief Legal Officer and compliance official for all Equifax entities.

28. To remain separate and distinct for the purposes of liability in this action, Defendants must operate as separate and legally as well as operationally distinct entities. Here, for matters and functions alleged and relevant herein, EIS and ECS were merely alter egos of Equifax, Inc. For purposes of how consumer data was handled, warehoused, used and sold, the corporate lines were disregarded in practice. EIS and ECS were mere instrumentalities for the transaction of the corporate consumer credit business. The Defendants shared full unity of interest and ownership such that the separate personalities of the corporation and subsidiaries no longer existed.

29. Further, recognition of the technical corporate formalities in this case would cause an irremediable injustice and permit Equifax, Inc. – the entity whose management ran, caused and permitted the events alleged herein – to defeat justice and to evade tort responsibility. *Heyde v. Xtraman, Inc.*, 199 Ga. App. 303, 306, 404 S.E.2d 607 (1991).

30. Accordingly, for all purposes hereafter, when the Plaintiffs allege "Equifax" as the actor or responsible party, they are alleging the participation and responsibility of all three Defendants collectively.

IV. FACTS

Equifax Breached its Duty of Care in Causing and Permitting the Data Breach

31. Equifax's business is information. It gathers, through third-party submissions and by accessing public and other records, information on nearly every American adult. It sells this information to countless businesses so that they may make decisions such as whether to grant credit, offer employment, loan money, issue insurance, rent housing, and the like. Equifax is strictly governed by the FCRA, but also holds common-law obligations to secure the information it possesses and protect it from unauthorized dissemination.

32. Equifax is aware that it is held to a heightened duty of care to protect its consumer file information. The text of its governing statute, the FCRA, itself warns Equifax of its "grave responsibilities" to maintain the privacy of consumer data, language that has been often repeated in court decisions in which Equifax was involved. And the Defendants even acknowledge in their 2016 Annual Report that, "We are subject to a number of U.S. and state and foreign laws and regulations relating to consumer privacy, data and financial protection. These regulations are complex, change frequently, have tended to become more stringent over time[.]"

33. The standard duty of care for Equifax was significant. It possessed – for profit and resale – the very private personal identifiers and financial information on nearly every consumer in the nation. In fact, Equifax possesses significantly greater amounts of that information than even the Federal and State governments, which themselves have to purchase reporting products from Equifax to discover such information. The standard for Equifax's maintenance and monitoring of its systems is much greater than an ordinary business.

34. The Gramm–Leach–Bliley Act ("GLBA"), 15 U.S. Code § 6801, and the regulations promulgated thereunder also imposed a duty on Equifax to insure the security and

confidentiality of customer records and information, to protect against hazards including unauthorized access or use, and to notify affected customers as soon as possible of any breach of security.

35. Equifax owed these duties, in particular, to Plaintiffs and Class Members, as persons whose personal identifying information ("PII") and other information was in Equifax's possession.

36. Equifax had a special relationship with the Plaintiffs and Class Members because it was entrusted with their personal information. Equifax's ability to acquire Class Members' PII and other information from them and other entities, created an independent duty of care because it was predicated on the understanding, based on Equifax's own representations, that Equifax would take adequate security precautions.

37. Further, Equifax's trade in the private and critical financial information of consumers poses an abnormally dangerous risk of financial harm to those consumers.

38. EIS is the entity that Equifax uses to warehouse and administer the retail credit information and credit reporting function for U.S. consumers. It gathers the information from third parties it labels "subscribers," referred to as "furnishers" under the FCRA, builds files matching that data to specific consumers and stores it in a database it titles "ACRO."

39. Separately, Equifax maintains the ACIS database which includes all documents created or obtained by Equifax from consumer contacts, such as consumer disputes, requests for a copy of the consumer's own credit file, correspondence sent to the consumer, and substantial amounts of data generated to document and archive each of these contacts. Communications that come in from the Equifax Internet portal that was the conduit for the data breach are maintained in the ACIS system. And Equifax has tried to convince the public generally that its "core database"

was not breached. But that distinction is meaningless as entry into the ACIS system provides access to nearly all of the same data – personal identifiers, accounts, etc. – that would be useful from the ACRO database. And access through ACIS gets a user directly into other data troves containing comparable information.

40. In the modest amount of information that it has released publicly, Equifax admits that its security team first observed suspicious network traffic associated with its U.S. online dispute portal web application no earlier than July 29, 2017 and continuing overnight into July 30, 2017.

41. Equifax cannot state with any certainty when this intrusion began.

42. Equifax has represented that the Data Breach occurred when hackers entered its dispute portal through a vulnerability via something called "Apache Struts."

43. Apache Struts is an open-source application framework that allows applications to run on a web server.

44. At a high level, an application framework can be thought of as "prepackaged" computer code that is specifically designed to allows users to then write their own custom code, add it to the environment, and then allow the prepackaged code portions to run the custom code portions so that in house programmers do not need to reinvent the wheel every time they build an application.

45. Since application frameworks are specifically designed to incorporate other pieces of code that are not part of the package (in this case, Apache Struts), they are particularly vulnerable to attack since the software is designed to and given permission to run code portions that are custom designed by in house programming teams (or in this case, outsiders).

46. The particular vulnerability with Apache Struts that was exploited in this case

allowed outsiders to run their custom code packages while they were uploading a file.

47. When this general Apache Struts vulnerability first became public knowledge in early March 2017, it was deemed a "0 day" exploit. This means that hackers became aware of the vulnerability before the developers of the software did.

48. Accordingly, a patch was released on March 7, 2017 and available publicly for download as a "critical patch."

49. The patch was rated with a NIST score of "10" meaning that on a 1-10 scale, this was the most critical type of vulnerability known to the developers.

50. Notwithstanding that the particular vulnerability in Apache Struts was identified and disclosed by U.S. CERT in early March 2017, Equifax failed to successfully apply the "patch" to its systems that would have fixed the problem.

51. Between March 7, 2017 and July 29, 2017, Equifax did not successfully apply the patch, if it even attempted to at all.

52. Equifax admits that the unauthorized accesses to certain files containing personal consumer reporting information occurred between, at least, May 13, 2017 through July 30, 2017. Equifax is also unable to rule out that the problem may have started even earlier during a separate successful and similar hack in March 2017 of its payroll subsidiary TALX (responsible for its "Work Number" payroll information product that Equifax markets to employers and data brokers).

53. The information obtained from TALX, particularly W-2 information stolen just before tax season, was likely a gold mine to those intruders as it allowed them to file false income tax returns.

54. Form W-2 information frequently sells in the range of $40 to $50 per individual between criminals on the internet.

55. Following a review by Mandiant, an outside security company that also investigated the March 2017 TALX breach but somehow still failed to correct this vulnerability, Equifax concluded that personal information relating to 143 million U.S. consumers – primarily names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers were breached, in addition to credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with credit and other personal identifying information for approximately 182,000 U.S. consumers.

56. Since the breach, sources have reported that personal identifying information accessed during the breach, including addresses, social security numbers, dates of birth and driver license numbers for various celebrities and public figures are presently offered for sale on the "Dark Web."

57. The Dark Web is a portion of the internet that is not accessible with traditional web browsers or through conventional search engines, but allows users with the proper system configuration to anonymously browse hidden websites and communicate with each over via highly encrypted messaging protocols.

58. While the Dark Web and its associated "TOR" browser technology is widely used by criminals to traffic in various categories of illicit materials, including drugs, firearms, professional hitman services, child pornography, and now apparently the private financial information of most of the adult population of the United States of America previously maintained by Equifax.

59. On September 20, 2017, Comodo Threat Intelligence Labs reported its findings that the individuals that breached Equifax's system also injected malware into the system that was successful in obtaining the login names and passwords of the highest executives at Equifax.

60. Using these credentials, the intruders were also able to exploit other services used by Equifax, such as Dropbox and LinkedIn.

61. After obtaining the stolen credentials on the Dark Web and reviewing them, Comodo found that Equifax's chief privacy officer, chief information officer, vice president of public relations, and vice president of sales used passwords with major security deficiencies such as all lowercase letters, no special symbols, and easily guessable words like spouses' names, city names, and even combinations of initials and birth years.

Equifax Refuses to Disclose the Fraudulent Procurement of Consumer Files

62. Despite knowing about the breach in July, Equifax kept the information secret. It did not reveal to individual consumers to whom it owed a contractual duty under a credit monitoring service. And it did not reveal to the public—those whose information was stolen and who stand to be injured from the breach—that the breach took place until September 8, 2017. But even then, Equifax has not disclosed exactly who was affected and what information was accessed.

63. The credit report information fraudulently procured from Equifax is all that is necessary to fraudulently obtain credit, tax returns and even a driver's license. With this information, an identity thief can now open credit, obtain full credit files from other CRAs, and even verify the falsified identity in future transactions.

64. Plaintiffs and Class Members will incur costs associated with time spent and the loss of productivity from addressing and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance,

and annoyance of dealing with all issues resulting from the Data Breach; as well as damages to and diminution in value of their personal and financial information entrusted to Equifax.

65. And Equifax knows this, as well as the urgency of providing detailed information to victim consumers as soon as possible. It warns on its marketing site, "More than ever before, your employees and customers are at great risk for identity theft and fraud. Over 165 million data records of U.S. residents have been exposed due to data breaches since January 2005 - Privacy Rights Clearinghouse."[5]

66. Defendants (now ironically) boast of how effective and robust its data breach response time and program is, stating, "You'll feel safer with Equifax. We're the leading provider of data breach services, serving more than 500 organizations with security breach events every day. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market." *Id.* Such "industry leading" services and capabilities would, by Equifax's suggestion require the breached business to, "Quickly inform consumers[.]" *Id.*

67. Equifax has, however, not "quickly informed consumers" as to its own data breach. As of the date of this filing, Equifax still refused to substantively inform affected consumers. And Equifax waited at least six weeks before it publicly disclosed even the general fact of the data breach.

68. Customers who called the dedicated call center set up by Equifax were often unable to get a coherent or timely response.

69. Even the "free" credit monitoring it offered to hack victims came with a string. The Terms of Service for TrustedID (an Equifax owned company) contain a provision that an

5 http://www.equifax.com/help/data-breach-solutions/ (last visited September 21, 2017).

individual's "membership subscription may be subject to automatic renewal."[6] Offering credit monitoring to every American through TrustedID also positions Equifax to collect even more valuable PII. To sign up, a consumer must authorize TrustedID to retrieve information about the consumer from the other two credit bureaus (Equifax and TransUnion). The information on the credit reports of the bureaus can vary by up to 20%, meaning Equifax can gain access to, and ultimately profit from, additional information from the other two credit bureaus when consumers grant TrustedID access to their Equifax and TransUnion credit files.

70. The system Defendants implemented to update consumers about whether their credit reporting information had been procured by the identity thieves was ineffective and not helpful. To take advantage of this look up, all you need to do is provide your last name and last six (not 4) digits of your Social Security number. However, the website that Equifax launched often returned the same message to a user regardless of what information was put in.[7] And, the site is not hosted on the Equifax network and appears to be a website domain and structure that was previously recognized as critically vulnerable to a hack. Since trust is critical for web sites like this, especially after a breach of this severity, it is difficult for consumers to trust that Equifax latest online support option is properly protecting their data.

71. Regardless, even assuming the Class Members did not suffer a false positive; Equifax has still refused to provide any detailed information as to what specific data was procured for individual consumers. And the generalized summary of the fact that they produced data including personal identifying information and some credit card account numbers is of little comfort to Plaintiffs and Class Members. What specific documents or files were procured

6 https://www.trustedid.com/serviceterms.php?serviceterms (last visited Sept. 21, 2017).
7 https://www.riskbasedsecurity.com/2017/09/equifd-equifax-breach-response-off-to-a-rough-start/ (last visited September 21, 2017).

containing such information? What additional parts of the credit report file was obtained? Which database(s) were hacked and thus procured? What information does Equifax have as to who procured it?

COUNT I: BREACH OF DUTY OF CARE
Class Action Claim

72. Plaintiffs restate each of the allegations in the preceding paragraphs as if set forth at length herein.

73. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs brings this action for themselves and on behalf of a class (the "West Virginia Breach Class") defined as:

> All natural persons residing in West Virginia whose consumer reporting information at Equifax was procured as a result of the data breach announced by Equifax on or about September 7, 2017.
>
> The Class does not include Defendants' officers, directors, and employees; Defendants' attorneys; Plaintiffs' attorneys; any Judge overseeing or considering this action together with members of their immediate family and any judicial staff.

74. The class includes thousands of consumers and is so numerous that joinder of all members is impractical.

75. There are questions of law and fact common to the class, which common issues predominate over any issues involving only individual class members. For example, and without limitation: (a.) whether Equifax had a duty of care to maintain the security of class member credit reporting information; (b.) whether Equifax's duty was heightened; and (c.) whether Equifax breached that duty in its failure to secure class member data.

76. Plaintiffs' claims are typical of those of the class members. All are based on the same facts and legal theories. The tort alleged is the same and the class claim will rise and fall entirely based upon whether or not Plaintiffs' claim rises or falls.

77. The Plaintiffs will fairly and adequately protect the interests of the class. The Plaintiffs have retained counsel experienced in handling class actions and litigation against Equifax as well as involving consumer credit reporting data and privacy protections. Neither Plaintiffs nor their counsel have any interests that might cause them not to vigorously pursue this action. The Plaintiffs are aware of their responsibilities to the putative class and have accepted such responsibilities.

78. Certification of a class under Rule 23(b)(1) of the Federal Rules of Civil Procedure is proper. Prosecuting separate actions by or against individual class members would create a risk of adjudications with respect to individual class members that, as a practical matter, would be dispositive of the interests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests.

79. Certification of a class under Rule 23(b)(2) of the Federal Rules of Civil Procedure is appropriate in that Equifax has acted on grounds generally applicable to the class thereby making appropriate declaratory relief with respect to the class as a whole.

80. Certification of the class under Rule 23(b)(3) of the Federal Rules of Civil Procedure is also appropriate in that:

a. As alleged above, the questions of law or fact common to the members of the class predominate over any questions affecting an individual member. Each of the common facts and legal questions in the case overwhelm the more modest individual damages issues. Further, those individual issues that do exist can be effectively streamlined and resolved in a manner that minimizes the individual complexities and differences in proof in the case.

b. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Consumer claims generally are ideal for class treatment as they

involve many, if not most, consumers who are otherwise disempowered and unable to afford and bring such claims individually. Further, most consumers affected by Equifax's tortious conduct would likely be unaware of their rights under the law, or who they could find to represent them in federal litigation. Additionally, individual litigation of the uniform issues in this case would be a waste of judicial resources. The issues at the core of this case are class wide and should be resolved at one time. One win for one consumer would set the law as for every similarly situated consumer.

81. Equifax knew or should have known the risks inherent to its possession of massive amounts of sensitive personal information, including that (a) hackers would target Equifax, as a dominant player in the consumer credit reporting and data aggregation industry, in order to acquire such information; (b) the risk of sophisticated cyberattacks was continual and increasing; (c) its own lax protocols had resulted in prior data breaches; (d) measures were available to adequately address its cybersecurity deficiencies; and (e) failure to implement adequate cybersecurity practices would result in a data breach.

82. Equifax's conduct in failing to protect Class Members' information, as described above, constitutes negligence. Equifax had a duty to act as would a reasonable CRA to safeguard the personal financial information of consumers entrusted to it by federal and state statutes. Equifax breached that duty by failing to secure its systems, including but limited to, applying a simple security patch that had been released for months prior to the break-in, then failing for months to notify Class Members that their information was compromised. As a proximate result of this breach of duty, Class Members suffered injuries. Those injuries resulted in monetary damages to Plaintiffs and Class Members.

83. Equifax breached its duties to Plaintiffs and the Class through its conduct alleged herein. Equifax had the ability to protect Class Members' PII from the cyberattack resulting in the

Data Breach, but failed to do so. Equifax failed to implement reasonable or adequate data security practices to protect the type and scale of information in its possession, failed to timely detect the cyberattack, utilized outdated and otherwise improper security measures and techniques, failed to properly segment and patch systems containing sensitive consumer data, failed to disclose the flaws in its data security, and failed to provide timely notice of the Data Breach.

84. Equifax would have been able to prevent and/or limit the harm caused by the Data Breach had it maintained adequate protocols and security measures as alleged herein.

85. Defendants are also strictly liable for the data breach as Equifax owed a duty because of the uniquely heightened and financially dangerous nature of its business and business practices.

86. Plaintiffs and each class member has suffered actual harm and actual damages as a result of this breach, for which Plaintiffs seek remedy and judgment.

WHEREFORE, Plaintiffs demand judgment and relief as pled and as follows:

A. That an order be entered certifying the proposed Class under Rule 23 of the Federal Rules of Civil Procedure and appointing Plaintiffs and their counsel to represent them;

B. That judgment be entered against Defendants as pled for actual and punitive damages, as well as costs and reasonable attorney's fees;

C. That the Court grant disgorgement and other injunctive and declaratory relief as pled, and requiring Equifax to make full disclosures to Class Members;

D. That the Court grant such other and further relief as may be just and proper.

PLAINTIFFS DEMAND TRIAL BY JURY

By: */s/ Elizabeth Hanes*
Counsel

Elizabeth Hanes, # 10732
CONSUMER LITIGATION ASSOCIATES, P.C.
763 J. Clyde Morris Boulevard, Suite 1-A
Newport News, VA 23601
Telephone: 757-930-3660
Facsimile: 757-930-3662
elizabeth@clalegal.com